AWS SECURITY CERTIFICATION GUIDE

AWS Certified Security Specialty (SCS-C02)

Mastering Enterprise Cloud Security, Defense-in-Depth Architecture, and Exam Domain Objectives

Professional Cloud Security Series

Presentation Agenda

1. Core Foundations

AWS Shared Responsibility Model, Security Imperatives, and Certification Framework overview.

2. Technical Security Pillars

Identity & IAM, Encryption & KMS, Network Defense, Logging, Monitoring, and Threat Detection.

3. Practice & Strategy

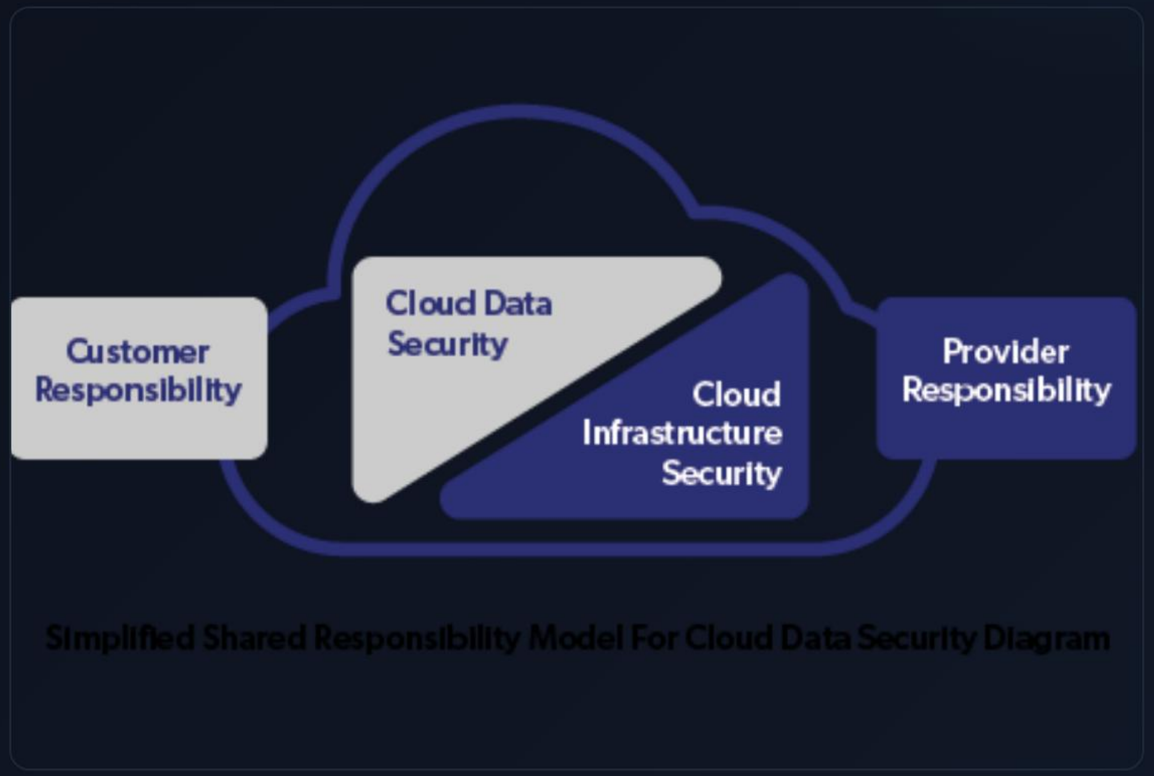
Common Security Pitfalls, Real-World Incident Response Scenario, Prep Roadmap, and FAQs.

PRESENTER NOTES

Welcome participants. This deck covers technical domain mastery for the AWS SCS-C02 exam alongside practical enterprise security strategies.

Why Enterprise AWS Security Matters

- **Rapid Attack Surface Expansion:** Dynamic cloud elasticity creates rapidly changing network perimeters.
- **Costly Misconfiguration Risks:** Publicly accessible S3 buckets and exposed API keys cause major breaches.
- **Regulatory & Compliance Mandates:** Strict enforcement of GDPR, HIPAA, PCI-DSS, and SOC2 standards.
- **Zero Trust Imperative:** Traditional perimeter security is replaced by continuous identity verification.



Simplified Shared Responsibility Model For Cloud Data Security Diagram

Key Cloud Security Challenges

Visibility Gaps

Shadow IT and unmonitored multi-region resources lead to blind spots in security oversight.

Privilege Creep

Over-provisioned IAM roles and excessive wildcard permissions invite credential compromise.

Alert Fatigue

High volumes of unprioritized security alerts obscure critical security threats.

PRESENTER NOTES

Solving these challenges requires moving from reactive patching to proactive, automated cloud security engineering.

Understanding AWS SCS-C02

65

Exam Questions

170 Minutes | Scaled Score: 100–1000 (750 to Pass)

Exam Purpose & Focus

The **AWS Certified Security Specialty (SCS-C02)** validates advanced technical expertise in securing AWS workloads, designing secure architectures, and implementing incident response mechanisms.

- Deep technical knowledge of AWS security native services.
- Ability to balance security tradeoffs against deployment complexity.
- Hands-on mastery of encryption, incident response, and governance.

Target Audience & Prerequisites

Target Role	Core Focus Area	Recommended Experience
Cloud Security Engineers	Infrastructure hardening, automated threat detection & response	2+ years AWS security hands-on
DevSecOps Specialists	CI/CD security integration, IAM automation, policy-as-code	2+ years cloud DevOps
Cloud Architects	Designing secure multi-account environments & landing zones	3-5 years enterprise cloud design
Compliance Specialists	Auditing AWS Config, GuardDuty, and compliance frameworks	2+ years cloud auditing

SCS-C02 Exam Domain Weightings

Domain weightings reflect balanced focus across design, operational monitoring, data privacy, and governance.

AWS Shared Responsibility Model

Customer Responsibility

"Security IN the Cloud"

- Customer Data & Data Classification
- Identity & Access Management (IAM)
- OS, Network & Firewall Configuration
- Client & Server-Side Encryption

AWS Responsibility

"Security OF the Cloud"

- Physical Security of Data Centers
- Hardware and Global Infrastructure
- Hypervisors & Host OS Isolation
- Edge Location Physical Defenses

Identity & Access Management (IAM)

- **Principle of Least Privilege:** Grant minimal permissions required for specific tasks using granular IAM conditions.
- **IAM Roles Over Static Credentials:** Avoid hardcoded long-term API access keys; enforce short-term credentials via STS.
- **Identity Federation & Identity Center:** Integrate SAML 2.0 / OIDC with Okta or Azure AD for single sign-on.
- **Service Control Policies (SCPs):** Implement central permission boundaries across AWS Organizations OUs.
- **IAM Access Analyzer:** Continuously analyze permissions to identify unintended public or cross-account access.

Encryption & Key Management (AWS KMS)

- **Symmetric vs Asymmetric KMS Keys:** KMS supports AES-256 symmetric and RSA/ECC asymmetric key pairs.
- **Automatic Key Rotation:** Enable annual automatic key rotation for AWS KMS Customer Managed Keys (CMKs).
- **Envelope Encryption:** Master keys encrypt Data Encryption Keys (DEKs), which encrypt large data payloads locally.
- **AWS CloudHSM:** Dedicated FIPS 140-2 Level 3 hardware security modules for strict regulatory requirements.

Security Logging & Monitoring

AWS CloudTrail

Records all API activity and management events. Enable multi-region organizational trails with S3 log-file integrity validation.

Amazon CloudWatch

Collects log streams, metrics, and custom alarms. Triggers EventBridge rules for automated security responses.

AWS Config

Continuously audits resource configuration history and evaluates compliance against desired security baselines.

Intelligent Threat Detection

AWS Security Service	Primary Detection Functionality	Key Data Sources
Amazon GuardDuty	ML-driven threat detection for compromised accounts & malicious IPs	CloudTrail, VPC Flow Logs, DNS, EKS, S3
AWS Security Hub	Central posture management & automated compliance checks	GuardDuty, Inspector, Macie, Config findings
Amazon Inspector	Automated vulnerability assessment & software package scanning	EC2 instances, ECR container images, Lambda
Amazon Macie	Data discovery & sensitive data protection (PII) using ML	Amazon S3 buckets

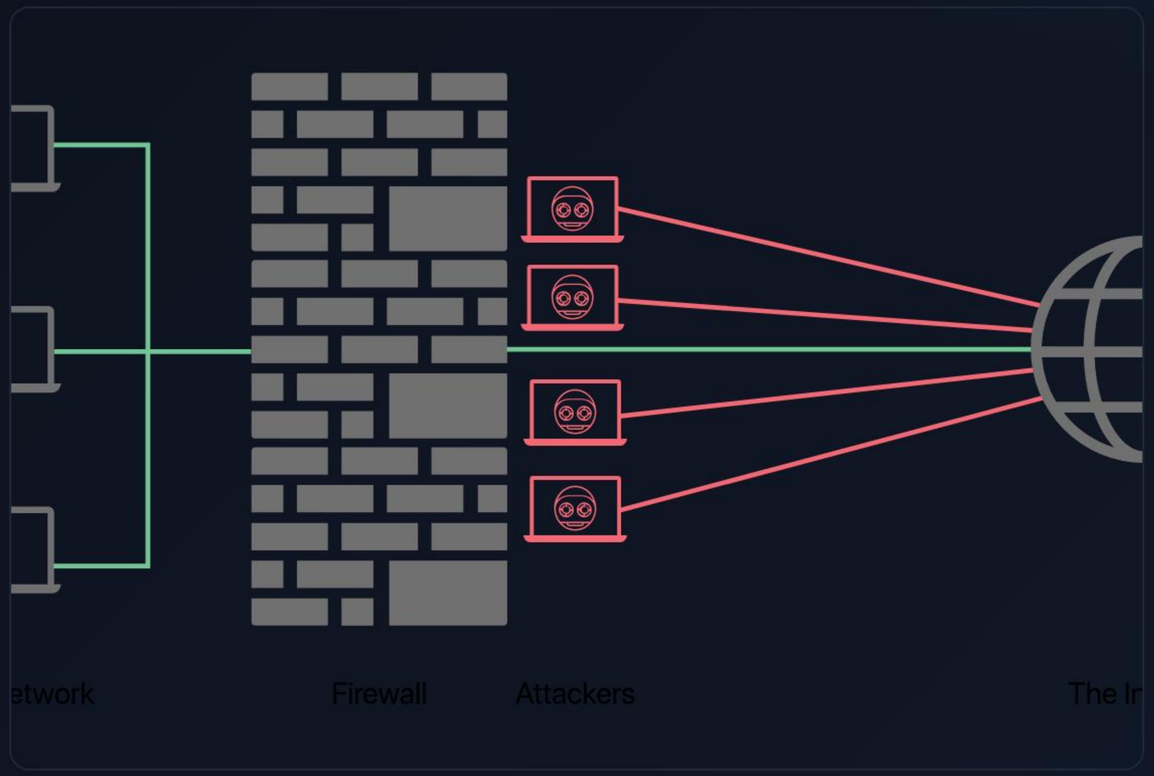
Infrastructure & Network Defense

VPC Microsegmentation: Combine stateful Security Groups (instance-level) and stateless NACLs (subnet-level).

AWS WAF: Protect web applications against Layer 7 OWASP Top 10 exploits and malicious bots.

AWS Shield Advanced: DDoS protection for Layer 3/4 and Layer 7 with DRT mitigation support.

AWS Network Firewall: Stateful inspection and intrusion prevention system (IPS) for VPC traffic.



Secrets Management Best Practices

AWS Secrets Manager

- Built-in automatic rotation for RDS, Redshift, and custom credentials via Lambda.
- Generates temporary database credentials dynamically.
- Fine-grained IAM policy access control and KMS encryption.

SSM Parameter Store

- Cost-effective storage for configuration values and SecureString parameters.
- Hierarchical parameter structuring and tagging.
- Integrated with KMS for encryption at rest.

Cloud Governance & Control

AWS Organizations

Centralized management of multiple AWS accounts with Service Control Policies (SCPs) enforcing guardrails.

AWS Control Tower

Automated landing zone creation with pre-configured guardrails for compliance and account provisioning.

AWS Artifact

On-demand access to AWS security compliance reports (SOC, PCI, ISO) and regulatory agreements.

Common AWS Security Mistakes

- ✕ **Using Root Account for Daily Operations:** Always lock root with hardware MFA and use IAM roles instead.
- ✕ **Open Security Groups (0.0.0.0/0):** Exposing SSH (22) or RDP (3389) ports to the public internet.
- ✕ **Disabling Logging in Secondary Regions:** Threat actors exploit unmonitored AWS regions.
- ✕ **Hardcoding AWS Credentials in Code Repositories:** Exposure of access keys in public GitHub repos.

Enterprise Security Best Practices

1. Zero Trust Identity

Mandate MFA everywhere, enforce short-lived credentials, and continuous IAM policy validation.

2. Universal Encryption

Encrypt all data at rest via KMS and in transit using TLS 1.3 across all services by default.

3. Automated Remediation

Deploy EventBridge rules and Lambda functions to instantly auto-remediate misconfigurations.

Real-World Scenario: Automated Incident Response

1. Detection

GuardDuty detects malicious crypto-mining on an EC2 instance.

2. Alerting

Findings published to Security Hub & EventBridge triggers Lambda.

3. Isolation

Lambda attaches restrictive isolation Security Group to target EC2.

4. Forensics

Automated EBS snapshot taken for analysis; alert sent to Slack/SNS.

Key Insight: Automated containment reduces Mean Time to Remediate (MTTR) from hours to seconds.

SCS-C02 Preparation Roadmap

Phase 1: Study Guide

Review AWS SCS-C02 Exam Guide, Official AWS Whitepapers, and Architecture Frameworks.

Phase 2: Hands-on Labs

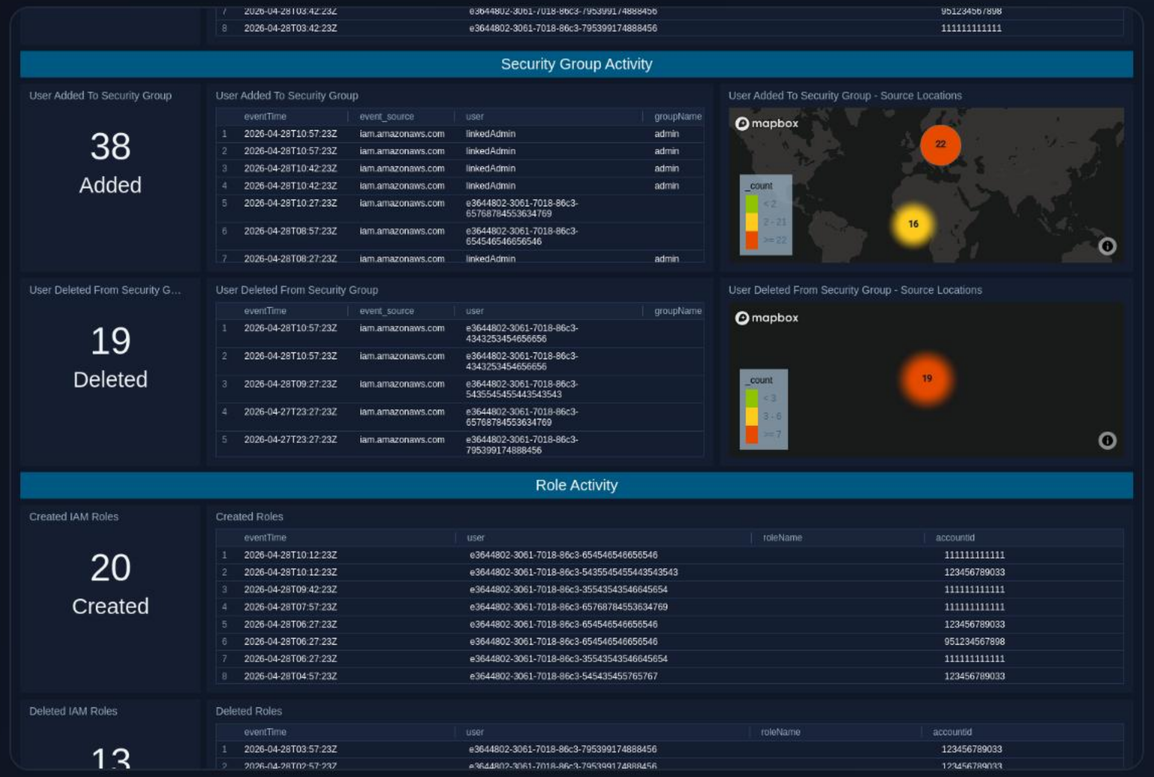
Build multi-account setups, configure GuardDuty, KMS key policies, and EventBridge automation.

Phase 3: Practice Tests

Solve practice questions, evaluate domain weaknesses, and practice time management.

Career Opportunities & Industry Demand

- **High Industry Demand:** Specialized cloud security credentials rank among the highest in IT value.
- **Target Industry Roles:** Senior Cloud Security Architect, DevSecOps Lead, Security Engineer.
- **Enterprise Impact:** Certified engineers lead security transformations and audit preparedness.



Key Presentation Takeaways

Defense-in-Depth

Combine IAM, network controls, encryption, and continuous monitoring for multi-layered defense.

Security Automation

Leverage EventBridge and Lambda to auto-detect and remediate threats dynamically.

SCS-C02 Validation

Earning the certification validates hands-on proficiency in enterprise cloud protection.

Frequently Asked Questions

How difficult is the SCS-C02 exam?

It is a challenging specialty-level exam requiring hands-on experience with complex scenarios.

Are there prerequisites for taking SCS-C02?

There are no formal prerequisites, but 2+ years of AWS security experience is highly recommended.

How often must I recertify?

AWS certifications are valid for 3 years, after which recertification is required.

Additional Learning Resources

AWS Skill Builder

Official digital training, practice question sets, and hands-on lab modules.

AWS Security Documentation

AWS Well-Architected Framework - Security Pillar whitepaper & security blogs.

Educational Resources

Explore specialized certification preparation courses such as the DevOpsSchool AWS SCS-C02 Guide for structured learning tracks.

Thank You!

Questions & Open Discussion

AWS Certified Security Specialty (SCS-C02) Presentation

Enterprise Cloud Security & Professional Certification Series

Image Sources

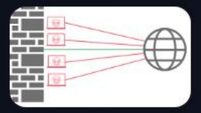
https://cpl.thalesgroup.com/sites/default/files/inline-images/cloud-data-security-diagram.png

Source: cpl.thalesgroup.com

---

https://dahqbtk1vlskk.cloudfront.net/wp-content/uploads/2025/08/03100048/iam-strategy-roadmap.webp

Source: www.zazz.io



https://www.cloudflare.com/resources/images/slt3lc6tev37/5wfmLijgWmcfy3AqBkmYKc/7d52f8a30aec966d734bf17a0f14573a/what-is-a-firewall.svg

Source: www.cloudflare.com

---

https://www.sumologic.com/help/img/integrations/cloud-security-monitoring-analytics/Amazon-CloudTrail-Security-Monitoring-Account-and-System-Monitoring.png

Source: www.sumologic.com